ธนัย อนันต์วัฒนาวิทย์

ไวรัส : สถานการณ์ล่าสุด

ติดตามสถานการณ์ความเคลื่อนไหวของไวรัสในปัจจุบัน

ไวรัสคอมพิวเตอร์ คือ มหันตภัยของผู้ใช้คอมพิวเตอร์เกือบทุกคน จากเมื่อประมาณสิบปีก่อนที่ไวรัสตัวแรกปรากฏขึ้นมา ปัจจุบันไวรัสได้มีการพัฒนาไปในทิศทางใดแล้ว น่ากลัวหรือว่าอันตรายมากน้อยเพียงใด ขอให้ลองติดตาม

ไวรัสคอมพิวเตอร์คืออะไร

มีหลายคนที่เข้าใจผิดกับคำว่าไวรัสคอมพิวเตอร์ คิดว่าไวรัสคอมพิวเตอร์คือโปรแกรมที่เขียนขึ้นมาเพื่อทำลายผู้อื่น แต่ความจริงแล้วนิยามของคำว่า ไวรัสคอมพิวเตอร์ที่ยอมรับกันในปัจจุบันจะหมายถึงโปรแกรมคอมพิวเตอร์ภาษาใดก็ได้ที่สามารถเพิ่มจำนวนชุดหรือสำเนาของตัวเองให้มากขึ้น เหมือนมีการขยายพันธุ์-แพร่พันธุ์ของสิ่งมีชีวิต โดยการเพิ่มจำนวนนั้นเกิดขึ้นด้วยกลไกของตัวโปรแกรมไวรัสเอง

ทั้งหมดนี้ไม่มีอะไรที่เกี่ยวกับการทำลายล้าง แต่ที่ไวรัสมีภาพลักษณ์ที่น่ากลัวเป็นเพราะผู้เขียนไวรัสบางกลุ่มได้แทรกคำสั่งในการทำความเสียหายไว้ในโปรแกรมด้วย หรือบางครั้งแม้ผู้เขียนไวรัสไม่ได้ตั้งใจให้เกิดการทำลาย แต่ด้วยข้อบกพร่องของการเขียนก็อาจทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์ที่ติดไวรัสได้

ประเภทของไวรัส

ไวรัสคอมพิวเตอร์ที่มีผู้เขียนและพัฒนากันมานั้น พอจะจัดแบ่งตามเทคนิคในการแพร่ได้ 4 แบบด้วยกัน คือ ไวรัสบูต ไวรัสไฟล์ ไวรัสมาโคร และไวรัสแบบผสม

แต่เดิมนั้นเทคนิคในการเขียนไวรัสจะมีอยู่เพียง 2 แบบ คือ ไวรัสแบบบูตกับไวรัสแบบไฟล์ ไวรัสแบบผสมนั้นจะเกิดมาภายหลัง หลังจากที่มีผู้พัฒนาให้ไวรัสตัวเดียวเป็นทั้งบูตและไฟล์ได้ ส่วนไวรัสมาโครจัดว่าเป็นไวรัสสายพันธุ์ใหม่ล่าสุดที่เพิ่งคิดค้นกันมาไม่นานนี้เอง

ไวรัสบูต อมตะนิรันดร์กาล

ไวรัสบูต (Boot Virus) เป็นไวรัสชนิดที่เขียนกันไม่ยากนักเพราะเทคนิคกลไกต่าง ๆ จะเป็นไปแบบง่าย ๆ แต่มีการแพร่พันธุ์ได้ค่อนข้างแน่นอน และหวังผลได้ ทำให้ไวรัสบูตเป็นไวรัสที่มีการแพร่กระจายที่กว้างขวาง

ตัวไวรัสบูตมักเป็นโปรแกรมขนาดสั้น ๆ ไม่เกิน 1 เซกเตอร์ของแผ่นดิสก์ (512 ไบต์) จะหลบซ่อนอยู่ในเซกเตอร์แรกของแผ่นดิสก์ที่เรียกว่าบูตเซกเตอร์ ซึ่งบูตเซกเตอร์นี่เองก็คือโปรแกรมที่เครื่องคอมพิวเตอร์จะโหลดลงไปในหน่วยความจำเป็นโปรแกรมแรกเพื่อเริ่มต้นการโหลดระบบปฏิบัติการต่อไป ปกติเครื่องคอมพิวเตอร์จะโหลดโปรแกรมบูตจากบูตเซกเตอร์ของฮาร์ดดิสก์ แต่หากในขณะนั้นมีแผ่นดิสก์อยู่ในไดรฟ์ A: เครื่องก็

จะบูตจากไดรฟ A: แทน นั่นคือจุดเริ่มต้นของไวรัสบูต

เริ่มต้นสมมติว่าเครื่องของเราไม่มีไวรัสอะไรอยู่ทั้งสิ้น และเราได้แผ่นดิสค์มาแผ่นหนึ่งที่มีไวรัสบูตแฝงมาด้วย แผ่นดิสค์นั้นเราอาจนำมาใช้งานเก็บข้อมูลอะไรได้ตามปกติ โดยไม่มีผลเสียอะไร แต่หากเมื่อใดที่เราลืมแผ่นดิสค์ที่มีไวรัสนั้นไว้ในตัวขับไดรฟ์ A: และเผลอไปบูตแผ่นนั้นเข้า เช่นตอนที่แผ่นค้างอยู่ที่ไดรฟ์ A: แล้วเรากดรีเซ็ต หรือปิดเปิดเครื่องใหม่ ไวรัสในแผ่นก็จะเริ่มทำงานทันที

เครื่องจะโหลดโปรแกรมจากบูตเซกเตอร์ของแผ่นดิสค์นั้นลงไปไว้ในหน่วยความจำ ซึ่งในกรณีของแผ่นนี้ มันก็จะเป็นโปรแกรมของไวรัสนั่นเอง หลังจากนั้นโปรแกรมในหน่วยความจำก็จะถูกเรียกให้ทำงาน หากเป็นโปรแกรมบูตปกติก็จะไม่มีปัญหาอะไร แต่หากเป็นโปรแกรมไวรัสมันก็จะเริ่มทำงานในสองเรื่อง หนึ่งคือฝังตัวลงไปในหน่วยความจำโดยอาจขโมยเนื้อที่มาบางส่วนประมาณ 1-4 กิโลไบต์ และสองคือหาทางแพร่ไปยังฮาร์ดดิสค์และแผ่นดิสค์อื่นเมื่อมีโอกาส แต่ปกติจะแพร่ลงฮาร์ดดิสค์ทันที โดยจะบันทึกไวรัสลงไปทับในบูตเซกเตอร์ของฮาร์ดดิสค์ ส่วนโปรแกรมบูตตัวจริงของฮาร์ดดิสค์ โดยมากไวรัสจะนำไปเก็บซ่อนไว้ในที่ว่างในฮาร์ดดิสค์

ในความจริงแล้วคำว่าบูตเซกเตอร์ของฮาร์ดดิสค์นั้น จะมีความแตกต่างจากคำว่าบูตเซกเตอร์ของแผ่นฟลอปปี้ดิสค์อยู่เล็กน้อย ตรงที่ฮาร์ดดิสค์หนึ่งตัวสามารถมีบูตเซกเตอร์ได้หลายชุด 1 ชุด สำหรับ 1 พาร์ทิชัน ดังนั้นในระบบของฮาร์ดดิสค์ จึงต้องให้มีบูตเซกเตอร์หลักขึ้นมาใหม่อีก 1 ชุด เพื่อคอยแบ่งแยกว่าจะให้บูตเซกเตอร์ของพาร์ทิชันใดทำงาน บูตเซกเตอร์หลักนั้นจะตั้งชื่อใหม่ว่า มาสเตอร์บูตเรคอร์ด เรียกย่อ ๆ ว่า MBR และบางครั้งจะเรียกว่า Partition Table Sector หรือเซกเตอร์ตารางพาร์ทิชัน เพราะที่เซกเตอร์นี้นอกจากเก็บโปรแกรมบูตไว้ส่วนหนึ่งแล้ว ยังมีข้อมูลตารางพาร์ทิชันอยู่ด้วย

ส่วนบูตเซกเตอร์ของแต่ละพาร์ทิชันก็ยังคงเรียกบูตเซกเตอร์เหมือนเดิม

ไวรัสชนิดบูตนั้นสามารถเขียนให้แพร่ติดที่ MBR หรือบูตเซกเตอร์ก็ได้ แต่ที่พบบ่อยคือจะติดที่ MBR เพราะเขียนได้ง่ายกว่า

หลังจากไวรัสได้แพร่ตัวเองไปติดในฮาร์ดดิสค์แล้ว ถัดไปก็จะปล่อยให้เครื่องคอมพิวเตอร์บูตต่อไปตามปกติ โดยที่ผู้ใช้ไม่รู้สึกตัวและใช้เครื่องต่อไปเหมือนปกติ แต่เมื่อใดเรานำแผ่นดิสค์มาใช้งาน ไวรัสที่รอจ้องจังหวะอยู่แล้ว ก็จะแพร่ติดแผ่นดิสค์นั้นทันที ไม่ว่าจะนำดิสค์มาใช้กี่แผ่นก็จะติดหมด ทั้งนี้เพื่อเป็นการเพิ่มจำนวนตัวเองและกระจายไปอยู่ในดิสค์ให้มากที่สุด ทำให้มีโอกาสที่ดิสค์หนึ่งแผ่นในจำนวนนั้นอาจถูกนำไปบูตในเครื่องคอมพิวเตอร์อื่นต่อไป

ตัวอย่างของไวรัสบูตที่เคยแพร่ระบาดอยู่ในเมืองไทย เช่น Beijing, Angelina, Print Screen และ Stoned เป็นต้น

ไวรัสไฟล์ซับซ้อนมากขึ้นเรื่อย ๆ

ไวรัสเก่าแก่อีกประเภทหนึ่ง ซึ่งเก่าแก่พอ ๆ กับไวรัสบูต คือไวรัสประเภทที่ติดกับแฟ้มโปรแกรม หรือที่เรียกว่าไวรัสไฟล์ (File Virus)

ในระบบของเครื่องพีซีนั้น แฟ้มโปรแกรมที่ไวรัสเกาะติดได้โดยมากจะเป็นแฟ้มที่มีนามสกุล .EXE กับ .COM แต่ก็มีไวรัสบางตัวเหมือนกันที่เขียนมาเพื่อติดกับแบตช์ไฟล์ (.BAT) แต่ไม่พบว่ามีการแพร่กระจายจริง ส่วนแฟ้มโปรแกรมนามสกุลอื่น เช่น SYS, BIN, OVL พบว่ามีการติดน้อยมาก

การเขียนโปรแกรมไวรัสประเภทไฟล์นี้ค่อนข้างจะยาก เพราะกลไกของการแพร่นั้นเกี่ยวเนื่องกับระบบปฏิบัติการหรือดอสอยู่มาก ต่างจากไวรัสบูตที่เขียนได้โดยออกแรงไม่มากนัก

การทำงานของไวรัสไฟล์โดยทั่วไปจะมีลักษณะคล้าย ๆ กัน คือเริ่มต้นเมื่อเราได้โปรแกรมที่มีเชื้อไวรัสติดอยู่ก่อนแล้วมาใช้งานโดยที่เราไม่รู้ (และคนที่ให้ก็อาจจะไม่รู้) ทันทีที่โปรแกรมที่ติดไวรัสนั้นถูกโหลดลงในหน่วยความจำเพราะเราสั่งรัน โปรแกรมส่วนที่เป็นไวรัสก็จะเริ่มทำงานก่อน ไวรัสจะฝังตัวเองลงไปซ่อนในหน่วยความจำทันที จากนั้นจึงค่อยไปทำงานตามโปรแกรมเดิมที่มันเกาะอยู่เหมือนกับไม่มีอะไรเกิดขึ้น

เมื่อถึงเงื่อนไขที่เหมาะสมที่ผู้เขียนไวรัสตั้งไว้ ไวรัสก็จะแพร่หรือก๊อบปี้ตัวเองไปเกาะติดกับแฟ้มโปรแกรมอื่น ๆ ในฮาร์ดดิสค์ของคอมพิวเตอร์เครื่องนั้น หรือเกาะติดกับโปรแกรมในแผ่นดิสค์ที่เราใส่เข้าไปในไดรฟ์ A: หรือ B: จนคอมพิวเตอร์เครื่องเดียวนี้อาจมีไวรัสไฟล์พันธุ์เดียวติดงอมแงมเป็นร้อย ๆ โปรแกรม วันใดที่เราก๊อบปี้โปรแกรมในเครื่องของเราไปให้คนอื่นใช้ หรือเราใช้เองแต่เป็นคนละเครื่อง ไวรัสในเครื่องของเราที่เกาะติดกับโปรแกรมที่ถูกก๊อบปี้นั้นก็จะไประบาดติดเครื่องใหม่ต่อไป

ไวรัสไฟล์ในปัจจุบันมีการระบาดที่น้อยลง เป็นเพราะมีการเปลี่ยนแปลงในเรื่องระบบปฏิบัติการ เดิมนั้นไวรัสแบบไฟล์จะต้องเขียนให้ทำงานกับโปรแกรมบนดอส ซึ่งมีอยู่ 2 รูปแบบ คือ COM กับ EXE ไวรัสบางตัวติดได้กับโปรแกรมทั้งสองแบบ แต่บางตัวก็ติดได้เฉพาะรูปแบบใดรูปแบบหนึ่งเท่านั้น แต่เมื่อมีการใช้งานวินโดวส์และวินโดวส์ 95 มากขึ้น โปรแกรมพวก COM กับ EXE ของดอสจึงถูกเรียกใช้งานน้อยลง ไวรัสก็แพร่น้อยลง

มีผู้เขียนไวรัสบางกลุ่มได้พยายามพัฒนาโปรแกรมไวรัสที่ติดโปรแกรม EXE ของวินโดวส์ (รูปแบบ NE) และวินโดวส์ 95 (รูปแบบ PE) แม้จะแพร่ได้จริงแต่ก็ไม่แพร่ระบาดในวงกว้าง เพราะธรรมชาติของการใช้โปรแกรมบนวินโดวส์ นั้นต่างจากดอสค่อนข้างมาก ของดอสเราสามารถก๊อบปี้โปรแกรมจากฮาร์ดดิสค์เราให้คนอื่นไปใช้งานต่อได้

แต่บนวินโดวส์การก๊อบปี้โปรแกรมที่ผ่านการติดตั้งแล้วจากฮาร์ดดิสก์ของเราไปติดตั้งใหม่บนเครื่องอีกเครื่องนั้นทำได้ยาก สู้ติดตั้งจากแผ่นต้นฉบับหรือแผ่น CD จะง่ายกว่า ทำให้วงจรชีวิตของไวรัสเหมือนถูกตัดขาด การแพร่ของไวรัสที่ออกแบบมาเฉพาะวินโดว์จึงมีในวงจำกัด

ไวรัสไฟล์ที่เคยแพร่ระบาดในเมืองไทยเรามีอยู่มากมายหลายตัว เช่น Jerusalem, Key Press, Die Hard II, Batman II และ DIR 2V เป็นต้น

ไวรัสมาโครยอดนิยมล่าสุด

ไวรัสประเภทใหม่ล่าสุดของวงการที่เพิ่งมีการคิดค้นกันขึ้นมาเมื่อประมาณเดือนสิงหาคม ปี 2538 คือไวรัสประเภทมาโคร (Macro Virus)

แต่ก่อนนั้นผู้ใช้เครื่องคอมพิวเตอร์ทั่วไปอาจจะกลัวไวรัสไปหมดทุกอย่าง จึงมักจะถามผู้เชี่ยวชาญว่า ไวรัสติดพวกแฟ้มข้อมูล เช่น แฟ้มฐานข้อมูล DBF แฟ้มเอกสารและแฟ้มรูปภาพได้หรือไม่ คำตอบที่ได้รับการยืนยันจากผู้เชี่ยวชาญทุกคนคือ เป็นไปไม่ได้ เพราะแฟ้มพวกนั้น "เอ็กซีคิวต์" หรือทำงานไม่ได้ มันไม่มีโปรแกรมอยู่ในแฟ้มพวกนั้น

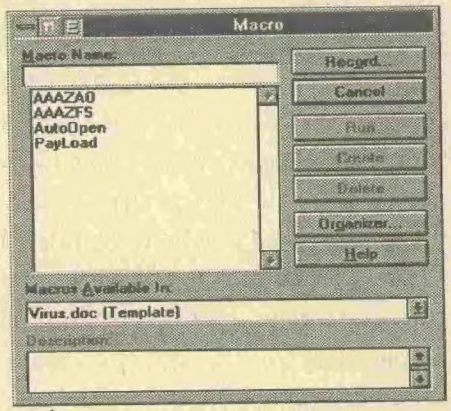
แต่เทคโนโลยีที่เปลี่ยนไปทำให้ผู้พัฒนาโปรแกรมสำเร็จรูปหลายกลุ่มเริ่มใส่ "คำสั่งง่าย ๆ" ปนไปกับแฟ้มข้อมูล เพื่อให้แฟ้มข้อมูลบางตัวสามารถควบคุมโปรแกรมสำเร็จรูปได้บ้าง เช่น มีการใส่คำสั่งมาโครไว้ในแฟ้มเอกสาร ใส่คำสั่งเอนิเมชันไว้ในแฟ้มรูปภาพ โดยไม่ได้นึกมาก่อนว่าจะเป็นจุดอ่อนให้นักเขียนไวรัสเข้าโจมตี

Concept คือไวรัสประเภทมาโครตัวแรกที่ปรากฏต่อหน้าสาธารณชน มันถูกเขียนมาจากคำสั่งของภาษา WordBASIC ที่อยู่ในโปรแกรมไมโครซอฟต์เวิร์ด รุ่น 6.0 แม้ว่าไมโครซอฟต์จะเรียกภาษาตัวนี้ว่าเป็นมาโคร แต่ในความจริงแล้ว WordBASIC เป็นสิ่งที่ใหญ่และเก่งกาจกว่าคำว่ามาโครมากนัก มันทำงานได้เกือบทุกอย่างที่ภาษาคอมพิวเตอร์ทั่วไปทำได้ รวมทั้งทำอันตรายให้กับระบบคอมพิวเตอร์

ไวรัสในรูปแบบใหม่ที่เรียกว่าไวรัสมาโครนี้ทำให้เกิดการแตกตื่นในเรื่องไวรัสคอมพิวเตอร์กันยกใหญ่ เพราะนี่ถือว่าเป็นการปฏิวัติเลยทีเดียว หลายคนวิเคราะห์ไวรัสมาโครแล้วพบว่ามันมีจุดน่าสังเกตอยู่หลายเรื่อง เช่น 1. ถือเป็นครั้งแรกที่พบไวรัสบน "แฟ้มข้อมูล" ในความรู้สึกของผู้ใช้ (แม้ว่าจริง ๆ แฟ้ม DOC ของ Word จะไม่ได้มีแต่ "ข้อมูล" เพียงอย่างเดียว) 2. ไวรัสมาโครไม่ได้ทำงานอยู่บนระบบปฏิบัติการ (DOS) ใด ๆ หากแต่ทำงานอยู่บนระบบปฏิบัติการจำลองของโปรแกรมสำเร็จรูปที่มันอาศัยอยู่ เช่น ทำงานบนระบบมาโครของไมโครซอฟต์เวิร์ด หากโปรแกรมสำเร็จรูปนั้นใช้งานบนระบบปฏิบัติการได้หลาย ๆ ระบบเช่น บน Windows, Windows 95, Windows NT, MAC OS หรือ OS/2 ไวรัสมาโครก็อาจจะสามารถแพร่และเติบโตบนโอเอสเหล่านั้นได้ด้วย และสามารถแพร่พันธุ์ข้ามไปมา เช่น จากพีซีไปยังแมค-อินทอชได้ 3. ไวรัสบนแฟ้มข้อมูลน่าจะมีโอกาสแพร่ได้มากกว่าไวรัสบนแฟ้มโปรแกรม เพราะปกติเรามักมีการส่งผ่านข้อมูลให้แก่กันมากกว่าการส่งโปรแกรม ยิ่งบนวินโดวส์ด้วยแล้ว แทบเป็นไปไม่ได้เลยที่จะมีการส่งโปรแกรมที่ติดไวรัสให้แก่กัน เพราะโปรแกรมมักจะมีขนาดใหญ่มากเกินกว่าจะก๊อบปี้ด้วยแผ่นดิสก์ได้

การทำงานของไวรัสมาโครที่ติดบน Word จะเริ่มจากเมื่อเราได้แฟ้มข้อมูล DOC จากเพื่อนของเราซึ่งติดไวรัสมาก่อนแล้ว มาเปิดอ่านในโปรแกรม Word ที่เครื่องของเรา ทันทีที่เปิดอ่าน มาโคร AutoOpen ที่แฝงตัวอยู่ในแฟ้มข้อมูลนั้นจะเริ่มทำงานและฝังตัวไวรัสมาโครไปยังแฟ้มมาโครกลางที่ชื่อว่า Normal.DOT จากนั้นก็จะอยู่เฉย ๆ รอเงื่อนไขในการแพร่สู่แฟ้มข้อมูลอื่น ๆ ต่อไป เช่น ให้แพร่เมื่อมีการสั่ง Save เป็นต้น หลังจากนั้น เมื่อเราเลิกใช้โปรแกรม Word คือสั่ง Exit ไวรัสมาโครก็จะหยุดทำงานไปพร้อมกับโปรแกรม Word ด้วย แต่เมื่อเราเรียก Word ขึ้นมาใหม่ครั้งใด แฟ้มมาโครกลาง Normal.DOT ก็จะถูกเรียกขึ้นมาใช้งานทุกครั้ง พร้อมกับไวรัสที่อยู่ในนั้น

ไวรัสมาโครเป็นไวรัสที่เขียนได้ไม่ยากนัก จึงมีผู้พัฒนาไวรัสประเภทนี้ขึ้นมามากจนนับได้เป็นร้อยสายพันธุ์แล้ว ทั้งที่เป็นไวรัสบน Word, Excel และ Ami Pro เช่นที่แพร่ระบาดในเมืองไทยก็มี Concept, Bandung, NPAD และ Laroux เป็นต้น



รูปที่ 1 Concept ไวรัสประเภทมาโครตัวแรกและเป็นไวรัสที่แพร่ระบาดในประเทศไทยมากที่สุดตัวหนึ่ง

ไวรัสผสม เป้าหมายคือการแพร่พันธุ์

ด้วยไวรัสแต่ละประเภทมีวิธีหรือช่องทางในการแพร่ที่แตกต่างกันไป ไวรัสบูตจะแพร่เมื่อมีการบูตเท่านั้น หากมีเหยื่อหลงเอาแผ่นดิสก์ที่มีไวรัสไปใช้งานแต่ไม่เคยบูตจากแผ่นดิสก์นั้นเลย ไวรัสบูตก็จะไม่สามารถแพร่พันธุ์ได้ ส่วนไวรัสไฟล์ก็แพร่ได้น้อยลงในระบบที่เป็นวินโดวส์หรือวินโดวส์ 95

เพราะเราไม่ค่อยจะก๊อบปี้โปรแกรมที่ใช้กับวินโดวส์แจกกันเท่าไรนัก และประเภทสุดท้าย ไวรัสมาโคร ก็จะแพร่ได้เฉพาะกับเครื่องที่ใช้โปรแกรมสำเร็จรูปเฉพาะตัว เช่น Word หรือ Excel เท่านั้น หากเครื่องไหนไม่ได้ใช้โปรแกรมเป้าหมายเหล่านั้นก็ไม่มีทางติดไวรัสเช่นกัน

นักเขียนไวรัสจึงเกิดไอเดียขึ้นมาว่าเอาไวรัสหลาย ๆ ประเภทมารวมกันเป็นตัวเดียวกัน น่าจะทำให้ไวรัสตัวนั้นมีโอกาสในการแพร่ได้ดีกว่าไวรัสธรรมดา

นี่คือต้นกำเนิดของไวรัสประเภทใหม่ Multi-partite Virus หรือไวรัสผสม ไวรัสที่เขียนมาให้สามารถแพร่ได้ในหลาย ๆ วิธี

ที่พบว่ามีการเขียนออกมามากที่สุดคือไวรัสผสมระหว่างไวรัสบูตกับไวรัสไฟล์ เพราะเทคนิคการเขียนไวรัสผสมนี้เกิดขึ้นมาก่อนที่จะมีการค้นพบเทคนิคของไวรัสมาโคร และอีกประการหนึ่ง ไวรัสมาโครนั้นเป็นไวรัสที่เขียนมาจากภาษาสูงและไม่เข้าพวกกับไวรัสบูตและไวรัสไฟล์ที่เขียนมาจากภาษาแอส-เซมบลี แต่ที่พบว่าเป็นไวรัสผสมระหว่างมาโครกับไฟล์ก็มีแล้วเหมือนกันคือ ไวรัส Nuclear แต่มีบักอยู่เลยแพร่ในแบบไวรัสไฟล์ไม่ค่อยได้

การทำงานของไวรัสผสมบูตกับไฟล์จะเป็นดังนี้ สมมติว่าไวรัสตัวแรกที่ได้มาเป็นไวรัสไฟล์ เมื่อเราสั่งรันโปรแกรมที่ติดไวรัส ไวรัสจะเริ่มต้นทำงานโดยฝังตัวเองลงในหน่วยความจำเหมือนไวรัสไฟล์ปกติ แต่จะแถมการก๊อบปี้ตัวเองทั้งหมดไปยังฮาร์ดดิสก์ของคอมพิวเตอร์นั้นพร้อมแก้ไข MBR หรือบูตเซกเตอร์ของฮาร์ดดิสก์ให้เป็นไวรัสบูตด้วย จากนั้นก็จะกลับมาทำงานเดิมของโปรแกรมที่ไวรัสเกาะอยู่ตามปกติ ขณะเดียวกันก็รอคอยการแพร่ไปสู่ไฟล์โปรแกรมอื่น ๆ และแผ่นดิสก์อื่น ๆ ที่ถูกนำมาใช้หลังจากนี้ จนกว่าจะปิดเครื่องคอมพิวเตอร์

ทีนี้เมื่อเรากลับมาใช้งานเครื่องใหม่ทันทีที่เราบูตเครื่องไวรัสส่วนที่เป็นบูตที่อยู่ในฮาร์ดดิสก์ก็จะเริ่มทำงานก่อนทันที โดยไวรัสจะฝังตัวในหน่วยความจำรอที่จะแพร่ลงแฟ้มโปรแกรมที่เราเรียกใช้งาน และแพร่ลงแผ่นดิสก์ที่เรานำมาเสียบเพื่ออ่านหรือเขียน

จะเห็นได้ว่าแผ่นดิสก์ทุกแผ่นที่นำไปใช้งานในเครื่องที่ติดไวรัสผสมนี้ สามารถแพร่ได้ทั้ง 2 วิธี ไม่ว่าผู้ที่ได้แผ่นดิสก์จะนำโปรแกรมในแผ่นดิสก์นั้นไปใช้งาน หรือนำแผ่นไปบูตเครื่องก็จะแพร่ไวรัสไปสู่เครื่องใหม่ได้ทันที ไวรัสประเภทผสมนี้จึงสถิติการแพร่กระจายได้ค่อนข้างมาก

ไวรัสแบบผสมที่มีแพร่ระบาดในบ้านเราก็มี OneHalf, 3783, NATAS และ 5K-4096 เป็นต้น

เทคนิคของคนเขียนไวรัส

นอกจากการแบ่งประเภทของไวรัสตามเทคนิคการแพร่แล้วยังมีชื่อแบบของไวรัสอีกบางคำที่ควรรู้จักไว้

Stealth Virus หมายถึงไวรัสที่มีความสามารถหลบซ่อนตัวจนโปรแกรมป้องกันไวรัส "ธรรมดา" ไม่สามารถหาตัวมันเจอได้ เช่น มีการหลอกว่าขนาดของแฟ้มที่ติดไวรัสมีขนาดเท่าปกติ หลอกว่าหน่วยความจำไม่หายไปไหน เป็นต้น

Polymorphic Virus หมายถึงไวรัสที่มีการแปลงตัวเองไปมาได้หลาย ๆ แบบ เหมือนกับจอมโจรพันหน้า ทำให้โปรแกรมป้องกันไวรัสไม่สามารถจดจำมันได้หมดในทุกรูปแบบ เวลาสั่งสแกนก็จะหาไม่เจอ หรือเจอก็จะเจอไม่ครบทุกแบบ

Non-resident Virus หมายถึงไวรัสที่ไม่มีการฝังตัวในหน่วยความจำ แต่จะแพร่ทันทีที่ถูกเรียกใช้งานในครั้งแรกและถอนตัวออกไปทันที การที่มันไม่ฝังตัวทำให้บางครั้งจะรอดจากการตรวจสอบของโปรแกรมป้องกันไวรัสได้ แต่มีจุดอ่อนตรงจะแพร่พันธุ์ได้ไม่มาก (ไวรัสปกติจะเป็น Resident Virus) ตัวอย่างของ Non-resident Virus เช่น XMas

Link Virus หมายถึงไวรัสไฟล์ที่ไม่ได้นำเอาโปรแกรมไวรัสทั้งหมดไปต่อเพิ่มให้กับโปรแกรมเหยื่อ แต่เก็บต้นฉบับโปรแกรมไวรัสไว้ในที่ปลอดภัยเพียงที่เดียวและชุดเดียว เวลาไวรัสจะทำงานก็มีกลไกในการนำเอาโปรแกรมไวรัสนั้นออกมาใช้ เช่น ใช้ตาราง FAT ของ OS เป็นตัวชี้ เป็นต้น การทำอย่างนี้ทำให้ขนาดของโปรแกรมเหยื่อไม่เปลี่ยนแปลง ตัวอย่างของ Link Virus ได้แก่ DIR II และ Byway เป็นต้น

Trojan horse ม้าไม้เมืองทรอย

มีโปรแกรมประเภทหนึ่ง ที่มีข่าวร่ำลือกันมาว่าเมื่อเรียกมาใช้งาน แค่ลองรันดูเล่น ๆ ก็อาจทำให้ข้อมูลในฮาร์ดดิสก์เสียหายได้ทันที โปรแกรมพวกนี้เราเรียกว่าโปรแกรมม้าไม้เมืองทรอย

ม้าไม้เมืองทรอยเป็นตำนานการรบระหว่างทหารกรีกที่เคลื่อนทัพไปตีเมืองทรอย แม้ว่าทหารกรีกจะล้อมเมืองทรอยอยู่เป็นเวลานานเกือบสิบปี แต่ก็ไม่สามารถเอาชนะทหารเมืองทรอยได้สักที จนสุดท้ายคิดกลอุบาย "ม้าไม้" ได้ โดยทหารกรีกได้สร้าง "ม้าไม้" ขนาดสูงใหญ่และสวยงามไว้ตัวหนึ่ง แล้วซ่อนทหารจำนวนหนึ่งไว้ในม้าไม้นั้น และทำทีว่าถอยทัพกลับโดยทิ้งม้าไม้ไว้ เมื่อชาวเมืองทรอยเห็นว่าทหารกรีกกลับไปหมดแล้วก็ได้ลากลูงม้าไม้นั้นเข้ามาในเมืองของพวกตน ด้วยเข้าใจว่าม้านั้นเป็นม้าศักดิ์สิทธิ์ ทำให้พวกตนชนะสงคราม ประกอบกับความอยากได้ของคนอื่นมาเป็นของตน พอตกดึกทหารที่ซ่อนตัวอยู่ในม้าไม้ก็ย่องออกมาจากม้าไม้และไปเปิดประตูเมืองให้ทหารกรีกเข้าโจมตีจนชาวทรอยต้องแพ้สงคราม

ในเรื่องของคอมพิวเตอร์ก็เช่นกัน มีคนไม่หวังดีบางคนเขียนโปรแกรมแกล้งคนอื่น เช่น เขียนโปรแกรมยูทิลิตี้หรือเกมที่เล่นได้จริง แต่ขณะกำลังเล่นก็จะแอบทำลายข้อมูลในฮาร์ดดิสก์ไปด้วย แล้วเอาโปรแกรมนี้ไปฝาก

แจกไว้ตามศูนย์ดาวน์โหลดต่าง ๆ เช่นใน BBS หรือในอินเทอร์เน็ต พร้อมเขียนคำโฆษณาเสียสวยหรู ผู้ที่ไม่รู้นึกว่าเป็นโปรแกรมที่ดีจริงก็ดาวน์โหลดหรือก๊อบปี้มาใช้ พอสั่งรันเท่านั้น ข้อมูลหายหมดทันที เหมือนกับชาวเมืองทรอยที่หลงไปลากจูงศัตรูเข้ามาถึงในเมืองของตัวเอง

โปรแกรมม้าไม้เมืองทรอย จะต่างจากไวรัสตรงที่โปรแกรมม้าไม้ไม่สามารถแพร่พันธุ์ได้จึงไม่ถือว่าเป็นไวรัส แต่ก็มีคนเข้าใจผิดบ่อย ๆ ว่าเป็นไวรัส

Hoax จดหมายลูกโซ่

สองสามปีมานี้ มีของเล่นใหม่ในวงการไวรัส เรียกกันว่า โฮกซ์ (Hoax)

โฮกซ์ คือ จดหมายลูกโซ่ที่มีการส่งแพร่กระจายด้วยอีเมล์ ภายในจดหมายจะมีข้อความที่ดูตื่นเต้นในเรื่องการพบไวรัสชนิดใหม่ที่เก่งกาจมาก และมีอันตรายเป็นที่สุด ตอนจบจะบอกให้ทุกคนระวังตนเอง และให้สำเนาจดหมายฉบับนี้ไปยังทุกคนที่เรารู้จัก เพื่อเป็นการเตือนคนที่เรารัก

ซึ่งหากเราเชื่อ ก็จะตกเป็นเหยื่อของโฮกซ์ทันที เมื่อเราส่งอีเมล์นี้ไปให้เพื่อนของเรา 3 - 4 คน เพื่อนของเราก็จะส่งต่อไปอีก 3-4 คน กลายเป็นจดหมายลูกโซ่วิ่งไปมาในอินเทอร์เน็ต

ตัวอย่างของโฮกซ์ที่หลายคนตกเป็นเหยื่อและคิดว่าเป็นเรื่องจริง คือจดหมายลวงเรื่องให้ระวังอีเมล์ที่มีหัวเรื่องว่า Good Times

ในจดหมายลวงที่เรียกว่า Good Times Hoax นี้จะบอกว่า ให้ทุกคนระวังอีเมล์ที่คุณได้รับในช่วงนี้ให้ดี หากอีเมล์นั้นมีหัวเรื่องว่า Good Times อย่าเปิดอ่านอีเมล์นั้นอย่างเด็ดขาด ให้ลบทิ้งทันที เพราะอีเมล์ฉบับนั้นเป็นไวรัสชนิดใหม่ที่แพร่ผ่านระบบการส่งอีเมล์ของอินเทอร์เน็ตได้ หากคุณเปิดอ่านมันจะลบข้อมูลในเครื่องของคุณจนหมด และขณะเดียวกันก็จะก๊อบปี้อีเมล์มรณะนั้นส่งไปตามรายชื่ออีเมล์ที่พบในเครื่องของคุณทันที ฉะนั้นขอให้คุณรีบเตือนเพื่อน ๆ ทุกคนที่รู้จักทางอีเมล์โดยส่งผ่านจดหมายฉบับนี้ไปยังเพื่อน ๆ โดยด่วน

ข้อความในจดหมายลวงนี้ดูเหมือนเป็นจริงเป็นจัง แต่ตราบถึงปัจจุบันก็ยังไม่มีใครสามารถสร้างไวรัสแบบที่ว่าไว้ในจดหมายนั้นได้จริง หรืออีกนัยหนึ่ง ไม่เคยมีใครได้รับอีเมล์ที่จ่าหัวว่า Good Times จริง ๆ เลยสักคน มีแต่ได้รับเจ้าโฮกซ์จดหมายลวงฉบับนี้เท่านั้น

เจ้าโฮกซ์ Good Times นี้ดังมากขนาดบางคนหลงเชื่อสำเนาอีเมล์ไปยังเพื่อนแล้วก็ยังไม่พอ ยังเอามาเขียนเป็นข่าวบ้าง บทความบ้าง ลงวารสารคอมพิวเตอร์และหนังสือพิมพ์ว่าให้ทุกคนระวังไวรัสชนิดใหม่ กว่าจะรู้ตัวว่าถูกหลอก ก็ทำเอาชาวบ้านผู้อ่านหลงเข้าใจผิดไปด้วยอีกเป็นหมื่นเป็นแสนคน ไม่เฉพาะเมืองนอก เมืองไทยก็หลงเชื่อเอาไปรายงานข่าวกันหลายฉบับ

นอกจาก Good Times แล้ว โฮกซ์ที่พอรู้จักกันในเมืองไทยก็มีอีกเช่น Deeyenda, Irina และล่าสุด AOL4FREE ข่าวลวงทั้งนั้น

ขอยืนยันว่าในขณะนี้ยังไม่มีอีเมล์ที่เป็นไวรัส (อนาคตไม่แน่ แต่ไม่ใช่เรื่องง่าย ๆ) จะมีก็แต่โฮกซ์เท่านั้น

อย่างไรก็ตาม อีเมล์ก็เป็นทางเผยแพร่ไวรัสได้เช่นกัน โดยการ "แนบ" หรือ Attach ไวรัสไปพร้อมกับอีเมล์

หากคุณเปิดอ่านอีเมล์ (ซึ่งไม่ต้องกลัวว่าจะติดไวรัส) แล้วพบว่ามีแฟ้มอะไรบางอย่างแนบมาพร้อมกับอีเมล์ ขอให้ระมัดระวังหน่อย ให้แกะแฟ้มที่แนบนั่นออกมาเป็นแฟ้มอิสระ แล้วใช้โปรแกรมป้องกันไวรัส สแกนดูสักรอบก่อนนำไปใช้งาน

แฟ้มที่แนบกับอีเมล์แล้วสามารถเป็นไวรัสได้ก็มีพวกแฟ้มโปรแกรม .COM, .EXE กับแฟ้มเอกสารของไมโครซอฟต์เวิร์ด .DOC, .DOT และไมโครซอฟต์เอ็กเซล .XLS

ดังนั้นเมื่อได้อีเมล์ที่มีแฟ้มนามสกุลต่าง ๆ ที่กล่าวมาแนบมาด้วยก็อย่าผลีผลามไปเปิดดูหรือเรียกใช้แฟ้มแนบเหล่านั้น ต้องใช้โปรแกรมป้องกันไวรัสตรวจสอบก่อนเสมอ

ไวรัสในอีเมล์

ผู้ใช้อินเทอร์เน็ต จำนวนไม่น้อยกลัวเจ้าสิ่งที่มีคนเล่าให้ฟังว่าเป็นอีเมล์ไวรัส กลัวเหลือเกินว่า พอเปิดอ่านอีเมล์แล้วไวรัสจะแพร่ติดเข้าเครื่องของตัวเองทันที

ไวรัสยอดนิยมปี 39

ในรอบปีที่ผ่านมา มีไวรัสมากมายที่เข้ามาแพร่ระบาดและทำความเสียหายให้กับผู้ใช้เครื่องคอมพิวเตอร์ในบ้านเรา บริษัท อาร์แอนด์ ดี คอมพิวเตอร์ ซิสเท็ม จำกัด ผู้ผลิต

ตารางที่ 1

ลำดับที่	ชื่อไวรัส	ประเภท	ขนาดของไวรัส (ไบต์)	แหล่งกำเนิด
1	DIE HARD II	ไฟล์	4,000	แอฟริกาใต้
2	3783	ผสม	3,783	ญี่ปุ่น
3	Batman II	ไฟล์	2,844	-
4	CONCEPT	มาโคร	ไม่มีข้อมูล	สหรัฐอเมริกา
5	Onehalf	ผสม	3,544	ออสเตรีย
6	NATAS	ผสม	4,744	สหรัฐอเมริกา
7	Beijing	บูต	512 (1 เซ็คเตอร์)	ไต้หวัน
8	Angelina	บูต	512 (1 เซ็คเตอร์)	-
9	Byway	ไฟล์	2,048	-
10	DIR 2 V	ไฟล์	1,024	บัลแกเรีย

และจำหน่าย Anti Virus Card ได้รวบรวมสถิติจากการแจ้งปัญหาไวรัสในประเทศไทยเป็นข้อมูลได้ดังตารางที่ 1

จากตารางแสดงรายชื่อไวรัสที่แพร่ระบาดมากที่สุดในประเทศไทยในรอบปี 2539 เฉพาะสิบอันดับแรก พบว่า DIE HARD II คือไวรัสที่มีการแพร่ระบาดมากที่สุด รองลงมาคือ 3783 และ Batman II แต่ที่มาแรงและคาดว่าปีนี้มาจะเป็นอันดับหนึ่งคือ ไวรัส CONCEPT ซึ่งเป็นไวรัสมาโคร สำหรับปี 40 นี้จะเป็นอย่างไรคงต้องรอดูกันต่อไป

การป้องกันไวรัสที่ได้ผล

การป้องกันไวรัสเป็นสิ่งจำเป็นที่ผู้ใช้คอมพิวเตอร์ทุกคนควรกระทำ ต่อไปนี้คือคำแนะนำในเรื่องการป้องกันไวรัสคอมพิวเตอร์

1. ศึกษาติดตามเรื่องไวรัสคอมพิวเตอร์ให้ใกล้ชิด การที่เราใกล้ชิดปัญหาย่อมทำให้เราป้องกันและแก้ปัญหาได้ดี

2. ให้คนรอบข้างรู้เรื่องไวรัสด้วย หากท่านมีเพื่อนที่ใช้เครื่องคอมพิวเตอร์ร่วมกับท่านหรือใช้คนละเครื่องแต่อยู่ในหน่วยงานเดียวกัน ควรให้ทุกคนรู้เรื่องไวรัสคอมพิวเตอร์ไว้ด้วย เป็นการช่วยกันป้องกันและลดช่องทางเข้าของไวรัสที่จะมาถึงเครื่องของท่าน

3. อย่าไว้ใจโปรแกรมทุกตัวที่ไม่ได้อยู่ในเครื่องของท่าน ปัจจุบัน CD เถื่อนเป็นสาเหตุหนึ่งของไวรัส อย่านำมาใช้ติดตั้งเพราะอันตรายมาก

4. ให้ระมัดระวังแฟ้มข้อมูลที่มีภาษามาโครอยู่ภายในได้ โดยเฉพาะอย่างยิ่งแฟ้มเอกสาร .DOC ของไมโครซอฟต์เวิร์ด

5. อย่าบูตเครื่องจากแผ่นดิสเกตต์โดยเด็ดขาด ให้บูตจากฮาร์ดดิสก์เท่านั้น เพื่อป้องกันไวรัสบูต

6. ควรจัดหาระบบป้องกันไวรัสมาใช้งาน เช่น โปรแกรมป้องกันไวรัส หรือแผงวงจรป้องกันไวรัส (Anti Virus Card)

7. แผ่นดิสก์โปรแกรมต้นฉบับต่าง ๆ ที่ซื้อมา จะต้องปิด Write Protect ทุกแผ่น และห้ามแกะออกโดยเด็ดขาด

อนาคตของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์คงไม่หมดไปจากวงการคอมพิวเตอร์แน่ ตัวเก่า ๆ อาจถูกฆ่าไปบ้างแต่ตัวใหม่ ๆ ก็ยังมีผู้เขียนออกมาอยู่ตลอด

บางตัวก็เป็นการลอกเลียนจากตัวเดิม บางตัวก็มีการปรับปรุงเล็ก ๆ น้อย ๆ และเมื่อถึงจุดหนึ่งก็มักจะมีไวรัสที่มีการใช้เทคนิคใหม่เอี่ยมออกมา ทั้งนี้เพราะสังคมของผู้เขียนไวรัสคอมพิวเตอร์ มักจะแสวงหาเทคนิคแปลกใหม่ แข่งกันนำเสนอความคิดของตนออกมา

เราในฐานะของผู้ใช้เครื่องคอมพิวเตอร์ ก็คงต้องติดตามข่าวคราวของไวรัสคอมพิวเตอร์กันต่อไป รวมทั้งต้องหาทางป้องกันตัวไปด้วย ทุกคนคงไม่มีใครอยากตกเป็นเหยื่อของเจ้าไวรัสจอมซนเหล่านั้น ขอให้ทุกคนโชคดีครับ

เมื่อคิดจะติดต่อกับ ISP

รายละเอียดเกี่ยวกับการให้บริการของ ISP ในประเทศไทย คุณสามารถสอบถามหรือหารายละเอียดเพิ่มเติมได้ดังนี้

1. ไอ-เน็ต ประเทศไทย
โทร. 642-7265-6
http://www.inet.co.th

2. อินเตอร์เน็ต เค เอส ซี
โทร. 576-0899
http://www.ksc.net.th

3. ล็อกซอินโฟ เซอร์วิส
โทร. 679-7890
http://www.loxinfo.co.th

4. สามารถไซเบอร์เน็ท
โทร. 937-0804
http://www.samart.co.th

5. เอ-เน็ต โทร. 861-1555
http://www.anew.co.th

6. เวิร์ลเน็ทเซอร์วิส โทร. 953-0303
http://www.wnet.net.th

7. เอเซียแอ็คเซส โทร. 617-0911
http://www.asianet.co.th

8. เทเลคอมโฮลดิ้ง โทร. 641-1818
http://www.asianet.co.th

9. ลายไทย อินเตอร์เน็ต เซอร์วิส
โทร. 310-5334-40
http://www.linethai.net.th

10. ไอเดียเน็ต โทร. 880-7080
http://www.idn.co.th

11. อินโฟนิวส์ โทร. 881-4700
http://www.infonew.co.th